

CC

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-173972

(43)Date of publication of application : 13.07.1993

(51)Int.Cl. G06F 15/00  
G06F 13/00  
H04L 9/06  
H04L 9/14

(21)Application number : 03-341012

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 24.12.1991

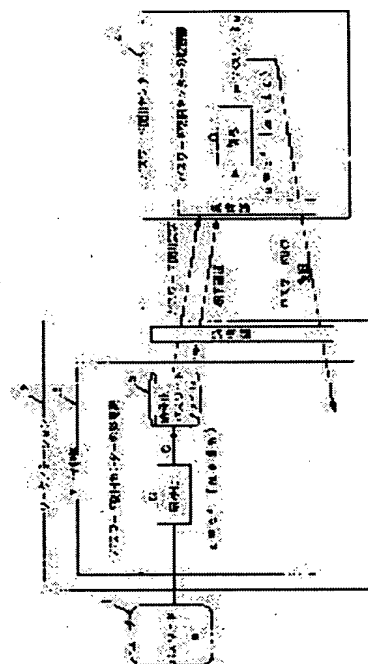
(72)Inventor : MATSUZAKI NATSUME  
TATEBAYASHI MAKOTO

## (54) PASSWORD RESTORING METHOD

## (57)Abstract:

PURPOSE: To provide a method for restoring a lost password and a method for confirming an inputted password without impairing safety nor easiness.

CONSTITUTION: A password restoration center 4 which restores the password is provided and a user ciphers his or her password by using the open key of the password restoration center 4 and then stores it. If the password is lost, the user indicates the ciphered and stored password and requests the password restoration center 4 to restore the password. The password restoration center 4 after certifying the user 1 deciphers the ciphered password by using a secret key and informs the user 1 of the result. Then the ciphered password is stored on a portable medium and identification information, etc., the user 1 is ciphered at the same time. The ciphered password is used to confirm whether or not the inputted password is correct.



## LEGAL STATUS

[Date of request for examination] 17.03.1997

[Date of sending the examiner's decision of rejection] 21.03.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平5-173972

(43)公開日 平成5年(1993)7月13日

(51)Int.Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 E	8219-5L		
13/00	3 5 1 Z	7368-5B		
H 0 4 L 9/06				
9/14				
	7117-5K		H 0 4 L 9/02	Z

審査請求 未請求 請求項の数6(全7頁)

(21)出願番号 特願平3-341012

(22)出願日 平成3年(1991)12月24日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74)代理人 弁理士 中島 司朗

(54)【発明の名称】 パスワード復旧方法

(57)【要約】

【目的】 ①安全性、簡易性を損なうことなく紛失したパスワードを復旧する方法を提供する。

②入力されたパスワードの確認方法を提供する。

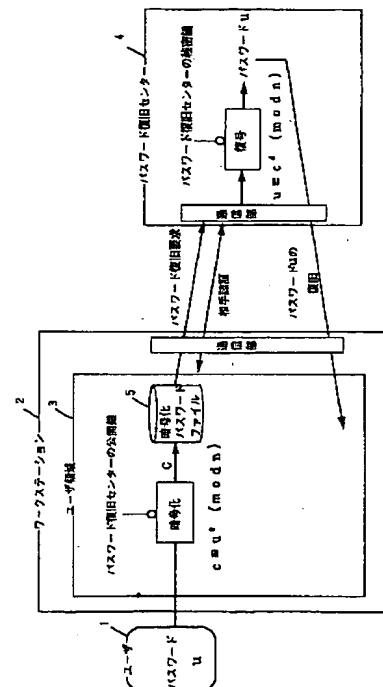
【構成】 ①パスワードの復旧を行うパスワード復旧センターを備え、ユーザは自分のパスワードをパスワード復旧センターの公開鍵を用いて暗号化した上で保管する。万一パスワードを紛失したときには、この保管している暗号化したパスワードを提示してパスワード復旧センターにパスワード復旧を要求する。パスワード復旧センターはユーザの認証を行った後、秘密鍵により暗号化パスワードを復号し、その結果をユーザに通知する。

②前記暗号化パスワードを可搬媒体に格納する。

③ユーザの識別情報等も同時に暗号化する。

④暗号化されたパスワードを入力されたパスワードの正否の確認に使用する。

【効果】



## 【特許請求の範囲】

【請求項1】 パスワード復旧センターが自己の秘密鍵を保持し、それに対する公開鍵をユーザに公開するステップと、ユーザが自己のパスワードを前記公開鍵を用いて暗号化し、その結果を暗号化パスワードとして保持するステップと、ユーザがパスワードを紛失した場合には前記暗号化パスワードを前記パスワード復旧センターに提示して前記パスワードの復旧を請求するステップと、パスワード復旧センターが前記提示された暗号化パスワードを前記秘密鍵を用いて復号するステップと、その復号結果をユーザに通知するステップとを有することを特徴とするパスワード復旧方法。

【請求項2】 前記暗号化パスワードを可搬媒体に保持することを特徴とする請求項1記載のパスワード復旧方法。

【請求項3】 前記パスワードに替えてパスワードとユーザ固有の識別情報との結合である結合パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項1若しくは2記載のパスワード復旧方法。

【請求項4】 前記パスワード若しくは結合パスワードに替えて、ユーザがパスワードに秘密処理を行った秘密パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項1若しくは2若しくは3記載のパスワード復旧方法。

【請求項5】 複数の、パスワード若しくは結合パスワード若しくは秘密パスワードが一個のパスワードとして暗号化され、暗号化パスワードとされることを特徴とする請求項1若しくは2若しくは3若しくは4記載のパスワード復旧方法。

【請求項6】 入力されたパスワードを前記パスワード復旧センターの公開鍵を用いて暗号化するステップと、このステップで得た暗号化パスワードと保持している前記暗号化パスワードとを比較することによって前記の入力値が正しいパスワードか否かを確認するステップとを有することを特徴とするパスワード入力 of の正否確認方法。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 パスワードを紛失した場合の復旧方法に関する。

## 【0002】

【従来の技術】 近年、開放的なワークステーションネットワークが普及する一方、ワークステーションで扱う情報の重要性が増してきている。これらのことを背景に、ワークステーション間のデータのやり取り、データベースの蓄積などに暗号化技術が導入されてきている。

【0003】 例えば、他者に見られたくない内容のファイルはユーザの設定した数値情報たるパスワード（鍵）で、暗号化した上で保管しておけばよい。この場合の暗号方式としては、その便利さ故に暗号化と復号に同じ鍵

を用いる共通鍵暗号方式が一般的に用いられている。この方式においては、パスワードを知っているユーザ本人だけが、ファイルを暗号化する際に用いたパスワードで暗号化ファイルを復号してもとの内容を得ることが出来るため、その安全性は高い。

【0004】 ところが、この場合に、もしユーザが自分の設定したパスワードを紛失してしまったなら、暗号化して保管しておいたファイルからもとの内容を復旧することができなくなる。又パスワードを個人認証に用いている銀行の預貯金オンラインシステム等においても、そのパスワードを紛失すると、カードを使った引き出し、預け入れ等が不可能になってしまう。そのため、従来はこの大切なパスワードを、紛失しないように例えば紙などに書き付けて携帯するか、ワークステーションのそばにおいておくというようなことがなされていた。

## 【0005】

【発明が解決しようとする課題】 しかし、このような紛失対策はシステムの安全性を損なうため、本来的には好ましくない。すなわち、安全性の面からパスワードはそれを設定した本人の記憶だけに蓄えられるべきである。といてユーザが自分の設定したパスワードを失念等することにより紛失してしまうのを完全に防止するのは困難である。ところで、ファイルシステムの場合、ファイルの内容が重要であればあるほど、安全性確保の面からパスワードは長くなりがち（桁が大きくなりがち）であり、また近年パスワードを多数使用することが多くなり、これらの面からも失念等しやすい。

【0006】 この場合、オンラインシステムを利用しての銀行への預貯金であるならば、パスワードやマネーカードを紛失しても、別途預貯金通帳と印鑑の提出等による復旧がなされ得る。しかし、再発行の手間は大変である。一方、LAN、通信回線等の開放的なワークステーションネットワークを利用するデータベースの蓄積等においては、いかなる手段を使用してももとの情報を復旧することはできない。しかるに、従来、安全かつ簡易に紛失したパスワードを復旧する対策が用意されていなかった。そのためワークステーションを利用してのデータベースの蓄積等においては、その便利さは認識されつつも暗号化システムがあまり普及しない原因となっていた。

【0007】 本発明は、安全かつ簡単なパスワードを復旧する方法を提供することにより上記問題点を解決する目的でなされたものである。

## 【0008】

【課題を解決するための手段】 上記目的を達成するため、請求項1の発明に係るパスワード復旧方法においては、パスワード復旧センターが自己の秘密鍵を保持し、それに対する公開鍵をユーザに公開するステップと、ユーザが自己のパスワードを前記公開鍵を用いて暗号化し、その結果を暗号化パスワードとして保持するステッ

3

プと、ユーザがパスワードを紛失した場合には前記暗号化パスワードを前記パスワード復旧センターに提示して前記パスワードの復旧を請求するステップと、パスワード復旧センターが前記提示された暗号化パスワードを前記秘密鍵を用いて復号するステップと、その復号結果をユーザに通知するステップとを有することを特徴としている。

【0009】請求項2の発明に係るパスワード復旧方法においては、前記暗号化パスワードを可搬媒体に保持することを特徴とする請求項1記載のパスワード復旧方法として、請求項3の発明に係るパスワード復旧方法においては、前記パスワードに替えてパスワードとユーザ固有の識別情報等の結合である結合パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項1若しくは2記載のパスワード復旧方法としている。

【0010】請求項4の発明に係るパスワード復旧方法においては、前記パスワード若しくは結合パスワードに替えて、ユーザがパスワードに秘密処理を行った秘密パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項1若しくは2若しくは3記載のパスワード復旧方法としている。請求項5の発明に係るパスワード復旧方法においては、複数の、パスワード若しくは結合パスワード若しくは秘密パスワードが一個のパスワードとして暗号化され、暗号化パスワードとされることを特徴とする請求項1若しくは2若しくは3若しくは4記載のパスワード復旧方法としている。

【0011】請求項6の発明に係るパスワード入力正否確認方法においては、入力されたパスワードを前記パスワード復旧センターの公開鍵を用いて暗号化するステップとこのステップで得た暗号化パスワードと、保持している前記暗号化パスワードを比較することによって前記別の入力値が正しいパスワードか否かを確認するステップとを有することを特徴としている。

【0012】

【作用】以上の構成により、請求項1の発明においては、ユーザから提示された公開鍵を使用して暗号化されたパスワードに対し、パスワード復旧センターが自己の秘密鍵を使用することにより復号をなし、その結果をユーザに通知することがなされる。

【0013】請求項2の発明においては、ユーザがパスワードを可搬媒体に保管する。請求項3に係る発明においては、結合パスワードが暗号化され、暗号化パスワードとされる。請求項4に係る発明においては、秘密パスワードが暗号化され、暗号化パスワードとされる。

【0014】請求項5に係る発明においては、複数の、パスワード若しくは結合パスワード若しくは秘密パスワードが暗号化され、暗号化パスワードとされる。請求項6に係る発明においては、入力されたパスワードを公開鍵を用いて暗号化したパスワードと、あらかじめ保持し

4

ている暗号化パスワードとの比較がなされることにより、入力されたパスワードの正否確認がなされる。

【0015】

【実施例】以下、請求項1の発明を実施例に基づき説明する。図1は本発明に係るパスワード復旧方式の一実施例の構成を示すものである。本図において、1はユーザ、2はユーザの用いている開放的なワークステーション、3はワークステーション内のユーザ1の領域、4はパスワード復旧センターである。パスワード復旧センター4はユーザのワークステーション2とは別の機関であり、ユーザのパスワードの復旧を行なう場合のみユーザとの情報交換を行う。以下、本図を用いて本実施例の動作を説明する。

【0016】まず、パスワード復旧センター4はある公開鍵暗号方式を決定し、この公開鍵暗号方式における秘密の数値情報たる秘密鍵を保持し、この秘密鍵に対する公開の数値情報たる公開鍵をユーザ1に公開する。本実施例では公開鍵暗号方式として、RSA暗号方式を用いている。本RSA暗号方式は、1978年にリベスト、シャミア、アドルマン、の3人によって提案された公開鍵暗号方式で、'アメソッド オブ オプティニグ デジタル シグネチャズアンド パブリックキー クリプトシステムズ'(R. L. Rivest, A. Shamir and L. Adleman: "A method of obtaining digital signatures and public key cryptosystems", Comm. of ACM, pp. 120-126 (FEB. 1978))に詳しく述べられており、我国の文献では池野 信一、小山 謙二 共著、電子通信学会発行「現代暗号理論」の第六章に説明されている。

【0017】なお、RSA暗号の要旨は以下の通りである。RSA暗号においては、暗号鍵は $(e, n)$ の組であり、復号鍵は $(d, n)$ である。暗号鍵は公開される。そして暗号化と復号アルゴリズムはそれぞれ、平文をM、暗号文をCとすると、

暗号化は  $C \equiv M^e \pmod{n}$

復号は  $M \equiv C^d \pmod{n}$

で表される。なお、 $\pmod{n}$ は整数C、Mをnで除したときの剰余を示す。上記式はフェルマーの定理より、 $e \times d \equiv 1 \pmod{m}$ とすることにより成り立つ。ここで、mはnのオイラー(EULER)の関数値であり、n以下かつnと互いに素な正整数の個数を表す。そして $n = p \times q$  (p, q: 素数)としたとき、mは $(p-1)(q-1)$ の最小公倍数となる。

【0018】そしてこのRSA暗号の安全性は、

(1) 暗号文Cと公開鍵eよりもとの平文Mが求められないこと。数学(整数論)でいう指数計算、通信学でいう離散対数問題の困難性により、nを十分大きく取ると、CよりMを求めることは困難となる。

10

20

30

40

50

5

(2) 公開鍵  $e$  より  $d$  が求められないこと。

【0019】数学における素因数分解の困難性により、 $n$  の素因数である  $p$ 、 $q$  を十分に大きくとることにより  $d$  を求めることは困難となる。による。以上のもとで、パスワードの暗号化と復号の手順を以下に示す。パスワード復旧センター4は、秘密の素数  $p$ 、 $q$  と両者の積  $n$  と  $e \times d \equiv 1 \pmod{m}$  を満たす  $e$ 、 $d$  を求めて、 $(p, q, d)$  を秘密情報として保持し、 $(n, e)$  をユーザ1に公開する。

【0020】ユーザ1は、自己の設定した秘密の数値情報たるパスワード  $u$  を上記パスワード復旧センター4の公開鍵を用いて以下の計算により暗号化する。その結果である暗号化パスワード  $c$  は、ワークステーション上のユーザ1の暗号化パスワードファイル5を作成して、これに格納して保管しておく。

$c \equiv u^e \pmod{n}$  ( $u$ : パスワード、 $c$ : 暗号化パスワード。) … (数1)

そして、この操作はユーザ1が新規にパスワード  $u$  を登録するとき、あるいはパスワードを更新するときに行われる。なお、ここでの暗号化パスワードファイル5はパスワード復旧センターの公開鍵で暗号化されているため、ワークステーション内の他のユーザに知得されたとしても、安全性が損なわれる危険性はない。すなわち、 $n$  と  $c$  と  $e$  とから  $u$  をもとめるは、非常に困難である。

【0021】さて、ユーザが使用している自己のパスワード  $u$  を万一紛失したときには、ユーザ1はこの保管している暗号化パスワードファイル5内の暗号化パスワード  $c$  を、ワークステーション及びパスワード復旧センターの通信部を経由してパスワード復旧センターに通知し、パスワードの復旧を要求する。パスワード復旧センターはユーザ1の認証、すなわち復旧を要求している者がたしかにユーザ1であることの確認、を行う。そして、自分の秘密鍵を用いて以下の計算を行ない、パスワード  $u$  を復旧し、その結果をユーザ1に送信する。

【0022】 $u \equiv c^d \pmod{n}$  … (数2)

なお、この場合にパスワード復旧センターとユーザ1との通信が公開ネットワークを利用する場合には、第三者の詐称に対する防衛が必要であり、このための認証方法についても種々発明がなされており、本出願人等も別途特願平3-199148号、特願平4-337125号にて出願をなしているが、これらは本発明の要旨には直接に関係しないため、その説明は省略する。パスワード復旧センターからの送信内容を受信したユーザ1はこの復旧されたパスワード  $u$  を用いて、新しいパスワードを設定し直し、暗号化パスワードファイル5を更新する。なお、同時に、もとのパスワードを用いて暗号化している暗号化ファイルがある場合は復旧されたパスワードを用いて復号し、その上で新しく設定したパスワードで新しく暗号化し直す操作も行う。

【0023】次に、この方法の安全性について説明す

6

る。まず、ユーザがパスワードを記憶している間は、ユーザの暗号化パスワードファイルは、ワークステーション2内のユーザ1の領域3に格納されている。その領域3はワークステーションに備わるアクセス管理メカニズムによりパスワード復旧センターがユーザとの間の通信手段を使用して知得することができないようになっている。そのため、パスワード復旧センター4は、ユーザ1のパスワードを求めることはできない。また、ユーザ1が、暗号化パスワードを提示してパスワードの復旧を求めてきたときには、パスワード復旧センター4は自身の秘密鍵を用いてこれを復号し、ユーザ1のパスワードを得ることはできる。しかしながら、復旧したパスワードをユーザ1に送信した時点で、ユーザ1によりこのパスワードは変更されてしまう。

【0024】また、たとえ復旧センター4が悪意を有しており、復旧したパスワードを用いてユーザ1にそれを通知する前にユーザ1が紛失前のパスワードを使用して暗号化しているファイル5を得ようとしても、このファイル5はワークステーション2からのアクセス制御により外から得ることはできないので、内容が知られることはない。

【0025】次に、請求項2の発明について説明する。請求項1の発明に係る上記実施例では、ユーザ1が暗号化パスワードファイル5をワークステーション2内に保持するものとしていたが、例えばフロッピーディスクなどの可搬な媒体(図示せず)に格納して保管することが考えられる。このことによりユーザ1が自己のパスワードを紛失していない状態でのパスワード復旧センター4から暗号化パスワードへのアクセスがより一層困難になる。このような媒体に格納することによって、ユーザの暗号化パスワードの管理も容易になり、更に安全性が向上する。

【0026】また、同じく上記実施例においては、ユーザ1は既存の通信手段を用いてパスワード復旧センター4と情報のやり取りを行うものとしているが、これを例えばフロッピーディスクのような可搬媒体を郵送する等物理的に搬送する方法で行ってもよい。次に、請求項3の発明を説明する。

【0027】本発明においては、請求項1の発明に係る上記実施例における(数1)、及び(数2)に示す演算の対象は、ユーザ1のパスワード  $u$  でなく、次に示すようにユーザ1の数値化された識別情報(ID)と、パスワードを列記した結合パスワードが用いられる。ここに、識別情報とは氏名、住所などパスワード復旧センター4によりユーザ1を特定できる情報である。

【0028】 $C' = (ID \parallel u)^e \pmod{n}$  ( $\parallel$  は結合を示す) … (数3)

パスワード復旧センター4は、この暗号化、パスワード  $C'$  を復号して得たユーザ1の識別情報を、復旧を要求しているユーザの識別情報と比較する。これにより、ユ

10

20

30

40

50

7

ユーザ1の暗号化パスワードを知得した他のユーザが、ユーザ1を詐称してセンターにパスワードの復旧を要求するという不正を排除しえる。

【0029】次に、請求項4の発明を説明する。本発明においては、請求項1の発明に係る上記実施例における、(数1)及び(数2)に示す演算の対象は、ユーザ1によりパスワードの最終桁に無意味な数字を付加することにより秘密化された秘密パスワードである。この場合、パスワード復旧センター4は、ユーザ1がそのパスワードの最終桁に無意味な数字を付加していることを知らないため、たとえユーザ1のワークステーションに接近したとしても、ユーザ1のファイルの内容を知得するのは困難となる。更にまた、ユーザ1が複数の復旧センターを利用してパスワードを2段に暗号化したり、又1のパスワードを分割し、各分割したパスワードを別個独立の複数の復旧センターの公開鍵を使用して暗号化し、復号は各々の復旧センターに依頼し、その上で復号結果を結合することにより紛失したパスワードを復旧するようにしてもよい。このことにより、更に安全性が向上するため、重要な秘密情報や大金を取り扱う場合に極めて有効であろう。

【0030】次に、請求項5の発明を説明する。本発明においては、請求項1の発明に係る上記実施例における(数1)及び(数2)に示す演算の対象は、ユーザ1が使用する複数のパスワード等である。これにより、単一の公開鍵を使用して複数のパスワードを保管することが可能となる。従って、業務の都合で多数のLAN、公開通信ネットワークを使用する者等や多数の銀行と取引が有る者等に便利である。

【0031】しかも、万が一悪意あるパスワード復旧センター4や第三者に暗号化されたパスワードが復号されたとしても、第三者等にとっては復号された個々のパスワードがどのシステムのパスワードか不明であるため、システムの安全性は向上する。ことに、請求項4の発明と組み合わせられた場合には、この効果は増大する。次に、請求項6の発明を説明する。

【0032】上記請求項1の発明に係る暗号化パスワードは、ユーザ1自身若しくはその利用機関においてパスワードとして入力された数値の正否をただちに確かめるために用いることもできる。すなわち、ユーザ1自身若しくはユーザ1の利用機関が、パスワードとして入力した数値をあらかじめ記憶させてある計算プログラムによりパスワード復旧センターの公開鍵をもちいて暗号化した上で表示させ、あらかじめユーザ1により設定の上ユーザ1のものとして登録済の暗号化パスワードと比較して、一致していれば本入力値は第三者でなく、実際にユーザ1により正しく入力されたパスワードであることを確認する。

【0033】以上、本発明を実施例を中心に説明してきたが、本発明は何も上記実施例等に限定されないのは勿

8

論である。すなわち、上記請求項1の発明の実施例ではパスワード復旧センターによる復旧にRSA暗号を用いる方式について説明したが、これは公開鍵暗号方式であればどのようなものであってもよいのは勿論である。他の公開鍵暗号方式としては例えばエルガマル暗号がある。このエルガマル暗号については「アパブリックキー・クリプトシステム・アンド・シグネチャスキーム・ベイスト・オン・ディスクリット・ログリズム」(T. E. ElGamal: 'A public key cryptosystem and signature scheme based on discrete logarithm', Proc. Cryptot 84)に詳しく述べられている。なお、上述の「現代暗号理論」には、このエルマガル暗号の他、他の公開鍵暗号方式が幾つか説明されている。さらに、上記実施例及び「現代暗号理論」では整数上の演算が用いられているが、例えば楕円曲線、有限体GF(P)上で定義された一次元Abel多様体(既約で非特異な種数1の射影代数曲線、標数≠2, 3の場合には $Y^2 = X^3 + aX + b$ と表される。ここにa, bはGF(P)の元)を用いた演算であってもよい。

【0034】また、例えばパスワードは数字でなく「特許庁」、「発明」等の単語であってもよい。また入出力兼用でなく、入力専用、又は出力専用のものであってもよい。識別情報は氏名、住所等でなく郵便番号や企業における従業員番号等の数値であってもよい。識別情報とパスワードの結合も、単に両者を列記するだけでなく、両者を数値情報化した上で掛け算をなす等の秘密処理があわせてなされてもよい。またファイルの具体的意味内容も各種の数値化された情報や銀行預金に限らず、第三者に知られたくない個人的なメモ等も包含するのは勿論である。

【0035】

【発明の効果】以上、説明したように請求項1の発明においては、パスワード復旧センターはユーザがパスワードを記憶している間はユーザの保持する暗号化パスワードを知り得ず、ユーザのパスワードを求めすることはできない。そしてユーザがパスワードの復旧を求めてきたときには、それまで用いていたパスワードを知り得るが、これをユーザに送信した時点でユーザはパスワードを変更してしまうためパスワード復旧センターによる不正は困難である。また、第三者が暗号化パスワードを知り得ても、それを復号できないためユーザのパスワードを知ることが困難である。このため、パスワードを使用した開放的ワークステーションのパスワードの紛失事故にたいする耐性、安全性が向上する。

【0036】請求項2の発明においては暗号化パスワードは、フロッピディスクのような可搬媒体に格納してそれを設定したユーザ本人が保持するため、よりシステムの安全性が高まる。請求項3の発明においては、ユーザ

50

固有の識別情報が含まれているため、暗号化されたパスワードを取得した第三者の詐称によるパスワードの復旧要請を排除することが可能となり、よりシステムの安全性が高まる。

【0037】請求項4の発明においては、暗号化され、復号されるパスワード自体に秘密化処理がなされるため、とくに公衆回線等開放的な通信ネットワークを使用し、復旧センターやその利用の信頼性に難がある場合にシステムの安全性が向上する。請求項5の発明においては、複数のパスワードを一体にして保管することが可能となるため、多数のパスワードを利用するユーザの利便性が向上する。

【0038】請求項6の発明においては、暗号化パスワードを、入力されたパスワードが真にその設定者により正しく入力されたものか否かをただちに調べるために用いることができ、システムの安全性、利用性が高まる。

また、第三者の目にふれ易い環境の下でも、パスワード入力者は入力した数値情報をあらかじめ記憶させてある計算プログラムにより暗号化した上で入力装置に表示させることにより、視覚により本当に自分が設定しているパスワードが正しく入力されたか否かを確認の上、次の操作に移る様なことも可能となる。このため、この面からもシステムの安全性、利用性が高まる。

【図面の簡単な説明】

【図1】本発明の一実施例におけるパスワード復旧方式の構成図である。

【符号の説明】

1. ユーザ
2. ユーザの使用するワークステーション
3. ワークステーション内のユーザ1の領域
4. パスワード復旧センター
5. 暗号化パスワードファイル

【図1】

